THE
AMERICAN
MATHEMATICAL MONTHLY.

Entered at the Post-office at Springfield, Missouri, as second-class matter.

VOL. IX. JUNE-JULY, 1902. NOS. 6-7.

THE ORDER OF A CERTAIN SENARY LINEAR GROUP.

By PROF. L. E. DICKSON, Ph. D.

In the March number of the MONTHLY, the writer determined the factors of the determinant D of a certain square matrix of order six:

$$(1) \qquad \begin{vmatrix} \mathrm{I} & \alpha & \beta & \gamma & \delta & \varepsilon \\ \beta & \mathrm{I} & \alpha & \delta & \varepsilon & \gamma \\ \alpha & \beta & \mathrm{I} & \varepsilon & \gamma & \delta \\ \gamma & \delta & \varepsilon & \mathrm{I} & \alpha & \beta \\ \delta & \varepsilon & \gamma & \beta & \mathrm{I} & \alpha \\ \varepsilon & \gamma & \delta & \alpha & \beta & \mathrm{I} \end{vmatrix}$$

It is readily shown that the product of two such matrices is a third matrix of the same form. Hence, if we assign to I, α, β, γ, δ, ϵ all sets of values in a given field, such that D does not equal 0, we obtain a set of matrices having the group property. The group may be represented concretely as a linear homogeneous group in six variables. It is proposed to determine the order of this group in the Galois Field of order p^n, designated $GF[p^n]$. We have only to find the number of sets of elements I, ..., ε such that D does not equal 0. It was shown in the MONTHLY that

$$(2) \qquad D=(\mathrm{I}+\alpha+\beta+\gamma+\delta+\epsilon)(\mathrm{I}+\alpha+\beta-\gamma-\delta-\varepsilon)\triangle^2,$$

$$(3) \qquad \triangle\equiv\mathrm{I}^2+\alpha^2+\beta^2-\mathrm{I}\alpha-\mathrm{I}\beta-\alpha\beta-\gamma^2-\delta^2-\varepsilon^2+\gamma\delta+\gamma\varepsilon+\delta\varepsilon.$$

If $p=3$, $\triangle$ is the difference of two squares, so that

$$D\equiv(\mathrm{I}+\alpha+\beta+\gamma+\delta+\varepsilon)^3(\mathrm{I}+\alpha+\beta-\gamma-\delta-\epsilon)^3 \qquad (\mathrm{mod}\,3).$$

For 3^{5n} sets of values of I, ..., ε in the $GF[3^n]$, the first factor vanishes. Similarly for the second factor. Both vanish simultaneously for 3^{4n} sets of values. Hence the number of sets for which D does not equal 0, *i. e.*, the order of G, is $3^{6n}-(2.3^{5n}-3^{4n})=3^{4n}(3^n-1)^2$.

For p not equal to 3, we set $A=\mathrm{I}-\alpha$, $B=\mathrm{I}-\beta$, $C=\gamma-\delta$, $D=\gamma-\varepsilon$.

Then $\triangle=(A^2-AB+B^2)-(C^2-CD+D^2)$, and the two linear factors of D become

$$f\equiv 3(\mathrm{I}+\gamma)-(A+B)-(C+D),\; f_1\equiv 3(\mathrm{I}-\gamma)-(A+B)+(C+D).$$

The sets I, γ, A, B, C, D for which $D=0$, fall into three classes:

f not equal to 0, f_1 not equal to 0, $\triangle=0$;
f not equal to 0, $f_1=0$; $f=0$,

the second class not occurring if $p=2$, since then $f=f_1$. The third class includes p^{5n} sets. If p is not equal to 2, the second class includes $p^{2n}(p^{3n}-p^{2n})$ sets, since it includes all sets for which

$$3\mathrm{I}-A-B=3\gamma-C-D \text{ not equal to } 0.$$

To determine the number of sets in the first class, let ω be a root of $\omega^2+\omega+1=0$. Since p is not equal to 3, ω^2 is not equal to ω. Then

$$\triangle=(A+\omega B)(A+\omega^2 B)-(C+\omega D)(C+\omega^2 D).$$

If ω belongs to the $GF[p^n]$, $A+\omega B$ and $A+\omega^2 B$ are independent elements of the $GF[p^n]$. Hence there are as many sets A, B, C, D making $\triangle=0$ as there are sets in the $GF[p^n]$ making $xy-zw=0$, viz.,* $p^n(p^{2n}+p^n-1)$.

If ω does not belong to the $GF[p^n]$, we set

$$(4) \qquad A+\omega B=X,\; C+\omega D=Y.$$

Since $\omega^{p^n}=\omega$, we have $\triangle=X^{p^n+1}-Y^{p^n+1}$.

We are to determine the number of elements X, Y of the $GF[p^{2n}]$ for which $\triangle=0$. Then $X=RY$ where R is one of the p^n+1 elements for which $R^{p^n+1}=1$. According as Y does not equal 0 or $Y=0$, we obtain $(p^n+1)(p^{2n}-1)$ sets or 1 set X, Y. By (4) each set determines uniquely a set A, B, C, D in the $GF[p^n]$. Hence there are

---

*This result may also be obtained by subtracting from $(p^n)^4$ the number of sets for which $xy-zw$ does not equal 0, which is the order $(p^{2n}-1)(p^{2n}-p^n)$ of the general binary linear group in the $GF[p^n]$.

$$(p^n+1)(p^{2n}-1)+1=p^n(p^{2n}+p^n-1)$$

distinct sets A, B, C, D for which $\triangle=0$.

Whether ω belongs to the $GF[p^n]$ or does not, the number of sets A, B, C, D making $\triangle=0$ is therefore $p^n(p^{2n}+p^n-1)$. It remains to determine for each set the number of elements I, γ for which f is not equal to 0, f_1 is not equal to 0. For p not equal to 2, this number is $(p^n-1)^2$ since $\mathrm{I}+\gamma$ and $\mathrm{I}-\gamma$ must take independently p^n-1 values. For $p=2$, $f=f_1$ and the number is $(2^n-1)2^n$.

The total number of sets I, α, ..., ε for which $D=0$ is therefore

$p^n(p^{2n}+p^n-1)(p^n-1)^2+p^{2n}(p^{3n}-p^{2n})+p^{5n}$ (if p is not equal to 2, p not equal to 3.)

$2^n(2^{2n}+2^n-1)(2^n-1)2^n+2^{5n}$ (if $p=2$).

Subtracting these numbers from p^{6n} and 2^{6n} respectively, we obtain the order of G. The results may be combined into the theorem:

The order of the group G in the $GF[p^n]$ is $p^n(p^n-1)^4(p^n+1)$ if $p>3$; $3^{4n}(3^n-1)^2$ if $p=3$; $2^{2n}(2^n-1)^3(2^n+1)$ if $p=2$.

Consider the group H the matrix of whose general transformation is derived from the matrix (1) by setting $\alpha=\beta$, $\gamma=\delta=\varepsilon$, the equal elements corresponding to the conjugate operators in the symmetric group g_6. The determinant D of this special matrix is the special group-determinant of g_6. Then

$$(5) \qquad D'=(\mathrm{I}+2\alpha+3\gamma)(\mathrm{I}+2\alpha-3\gamma)(\mathrm{I}-\alpha)^4.$$

For $p=3$, $D'\equiv(\mathrm{I}-\alpha)^6$, so that the order of H is $3^{2n}(3^n-1)$.

For $p=2$, $D'\equiv(\mathrm{I}-\gamma)^2(\mathrm{I}-\alpha)^4$, so that the order of H is $2^n(2^n-1)^2$.

For $p>3$, we determine the number of sets I, α, γ in the $GF[p^n]$ for which $D'=0$. These are of three classes:

f' not equal to 0, f_1' not equal to 0, $\mathrm{I}-\alpha=0$;
f' not equal to 0, $f_1'=0$; $f'=0$,

where $f'=\mathrm{I}+2\alpha+3\gamma$, $f_1'=\mathrm{I}+2\alpha-3\gamma$. For the first class, $\mathrm{I}=\alpha$, $3\alpha\pm3\gamma$ is not equal to 0.

If $\alpha=0$, γ has p^n-1 values; if α is not equal to 0, γ has p^n-2 values. Hence

$$(p^n-1)+(p^n-1)(p^n-2)=(p^n-1)^2$$

is the number of sets in the first class. For the second class,

$$\mathrm{I}+2\alpha-3\gamma=0,\ \gamma \text{ is not equal to } 0,$$

giving $(p^n-1)p^n$ sets. The third class contains p^{2n} sets. Hence

$$(p^n-1)^2+(p^n-1)p^n+p^{2n}=3p^{2n}-3p^n+1$$

is the total number of sets making $D'=0$. Subtracting this number from p^{3n}, we obtain $(p^n-1)^3$ as the order of H for $p>3$.

The group* H is an invariant subgroup of G. In view of the preceding results, the order of the quotient-group is

$$p^n(p^{2n}-1) \text{ if } p>3 \text{ or if } p=2;\ 3^{2n}(3^n-1) \text{ if } p=3.$$

This result for p not equal to 3 is in accord with the general theory of group-matrices† by which the quotient-group is seen to be simply isomorphic with the group of binary substitutions of determinant unity in the $GF[p^n]$. The latter is known to be simple if $p=2$, and to have the factors of composition $\frac{1}{2}p^n(p^{2n}-1)$ and 2 if $p>2$.

The University of Chicago, March, 1902.

*The group H is evidently simply isomorphic with the commutative group of ternary linear transformations whose general matrix is

$$\left\{\begin{matrix} 1 & 2\alpha & 3\gamma \\ \alpha & 1+\alpha & 3\gamma \\ \gamma & 2\gamma & 1+2\alpha \end{matrix}\right\}$$

†Frobenius, Burnside, Dickson. See the references in the *Transactions of the American Mathematical Society*, July, 1902.

"THE BETWEENNESS ASSUMPTIONS."

By DR. ELIAKIM HASTINGS MOORE.

Amongst mathematicians there is abiding interest in the foundations of geometry—at present, in particular, as to the projective axioms. These axioms constitute, for instance, the first two groups I, II of Hilbert's system of axioms.

In a paper "On the Projective Axioms of Geometry," published January, 1902, in The Transactions of the American Mathematical Society (vol. 3, pp. 142-158), I exhibited and developed a new system of projective axioms for geometry of three or more dimensions, comparing it with the systems of Pasch, of Peano, and of Hilbert, and in this connection proving the redundancy in Hilbert's system I, II of the axioms I 4, II 4.

In the April 1902 number of THE MONTHLY (pp. 98-101), under the title, "The Betweenness Assumptions," Dr. Halsted published a second proof of the redundancy of II 4, a proof due to Mr. R. L. Moore, a student of his. Dr. Halsted alluded to my earlier proof of the theorem in the statement: "Mr. Moore has no intimation that any one has ever tried to prove these theorems." (l. c. p. 100.)

I wrote to Mr. Moore explaining the situation, and congratulating him upon the beauty of his proof. The congratulatory part of this letter appears in an editorial note (p. 148) of the May 1902 number of THE MONTHLY.

The letter was as follows: